

## Kinga Piwowarska

doktorantka, Katedra Prawa Pracy i Ubezpieczeń Społecznych,  
Wydział Prawa, Administracji i Stosunków Międzynarodowych,  
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

# Czy nowe technologie zrewolucjonizują rynek pracy?

## Wprowadzenie

Rozwój technologii dosięga każdego z nas w wielu aspektach życia, np. medycyny, pracy, edukacji, nauki, techniki, motoryzacji, social mediów. W niniejszym artykule skupiam się na wpływie owej technologii na pracę. Czy nowe technologie i nowe formy pracy – m.in. telepraca, praca z zastosowaniem technologii informacyjno-telekomunikacyjnych (*ICT based work*), praca w ramach platform cyfrowych (*crowdworking*) – zrewolucjonizują rynek pracy? Rozważę też, czy wykorzystywanie nowych technologii przez pracodawcę czy przyszłego pracodawcę, m.in. w zakresie *background screening* (w tym *credit* i *criminal check*), pozyskiwania i wykorzystywania danych biometrycznych, zastosowania technologii identyfikacji radiowej (RFID) poprzez wszczepianie chipa dla kontroli pracownika czy usprawnienia procesów organizacyjnych u pracodawcy, nie stanowi nadużycia podmiotowego prawa do prywatności i wręcz nie narusza godności.

W opracowaniu odniosę nowe technologie stosowane na rynku pracy do Ogólnego Rozporządzenia o Ochronie Danych Osobowych z 27 kwietnia 2016 r.<sup>1</sup>, które weszło w życie 25 maja 2018 r. i wymusiło zmianę w wielu aktach prawnych, w tym w ustawie z 26 czerwca 1974 r. – Kodeks pracy<sup>2</sup>. Rozważę, jak obecnie kształtują się przepisy k.p. w zakresie rewolucji technologicznej oraz czy istnieją zawody, które są zagrożone wyparciem z rynku pra-

<sup>1</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz. UE L 119/1 (dalej: RODO).

<sup>2</sup> Dz.U. z 2018 r., poz. 917 (dalej: k.p.).

cy ze względu na automatyzację pracy, oraz *a contrario* – czy istnieją zawody przyszłości, które będą potrzebne za kilkanaście lat.

## Background screening

Już na etapie rekrutacji potencjalny pracodawca, szczególnie korporacyjny, wykorzystuje szereg nowoczesnych i rozwiniętych technologicznie narzędzi, żeby „prześwietlić” potencjalnego pracownika, tj. zweryfikować dane, m.in. w zakresie: wykształcenia, dotychczasowego przebiegu zatrudnienia, doświadczenia, umiejętności – które kandydat podaje w CV, zaświadczeniach i innych dokumentach. Pracodawca często chce też sprawdzić niekaralność, historię kredytową oraz jaką opinią cieszy się kandydat w danej branży, aby w przyszłości uniknąć niepotrzebnych problemów. Ma to miejsce szczególnie przy zatrudnianiu na kierownicze, menadżerskie i samodzielne stanowiska pracy.

Rekruterzy coraz częściej szukają informacji o kandydatach na pracowników w Internecie: na portalach społecznościowych czy branżowych serwisach (tzw. *media research*). Dochodzi do wirtualnych kontroli tożsamości, ponieważ Internet stanowi ogromne źródło informacji o potencjalnym pracowniku. Co więcej, aby pozyskać pracownika, rekruterzy na stronach internetowych czy portalach społecznościowych, np. LinkedIn, GoldenLine, Facebook, Gumtree, infopraca, umieszczają oferty pracy i poprzez tzw. profilowanie<sup>3</sup> wyszukują potencjalnych kandydatów. Informacje o danym stanowisku pracy trafiają do konkretnych, dopasowanych już do stanowiska użytkowników portalu. Jest to możliwe dzięki temu, że użytkownicy portali sami zamieszczają tam informacje o sobie.

W zakresie „prześwietlania” kandydata na pracownika (tzw. *background screening*, *background check*, *pre-employment screening*), pracodawcy współpracują z wyspecjalizowanymi podmiotami trzecimi, zajmującymi się weryfikacją informacji o kandydacie. Jednym z takich podmiotów jest platforma Screening.pl<sup>4</sup>, oferująca następującą usługę: potencjalny pracodawca zamieszcza ofertę pracy, np. na portalu internetowym, zainteresowany ofertą kandydat na pracownika wysyła mu CV, po czym potencjalny pracodawca odsyła

<sup>3</sup> Zgodnie z motywem nr 71 RODO profilowanie polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa.

<sup>4</sup> Właściciele twierdzą że jest to pierwsza tego typu działalność w Polsce. Zob. *O nas*, Screening.pl, <http://www.screening.pl> [dostęp: 15.05.2018].

kandydatowi login i hasło do konta na Screening.pl, a on już we własnym zakresie wypełnia formularz, załącza CV, ewentualnie inne dokumenty oraz wyraża zgodę na weryfikację przez Screening.pl w zakresie: danych osobowych, historii edukacji i zatrudnienia, funkcji i udziałów w spółkach, prowadzenia jednoosobowej działalności gospodarczej, karalności, posiadanych certyfikatów i kursów oraz wiarygodności i długów. W zależności od wyników weryfikacji, potencjalny pracodawca podejmuje decyzję o zatrudnieniu (bądź nie) danej osoby. Niewątpliwie taki proces pozwala uniknąć zatrudnienia niekompetentnych, niewiarygodnych oraz karanych pracowników, niekiedy z wiarygodnościami, co mogłoby wywołać negatywne konsekwencje dla pracodawcy w przyszłości.

Oczywiście kandydaci na pracowników również korzystają z dobrodziejstw nowej technologii, jakimi są ciągle rozwijające się środki masowego przekazu, szczególnie Internet, poprzez czytanie opinii i zapytania na forach, blogach czy komunikatorach o warunki pracy i wynagrodzenia u danego potencjalnego pracodawcy. Niewątpliwie jeszcze 20 lat temu takie praktyki nie były powszechne, jednak standard zatrudnienia coraz bardziej się podnosi, a co za tym idzie – świadomość przyszłych stron stosunku pracy również się zmienia.

Skoro na polskim rynku funkcjonują podmioty zajmujące się *background screeningiem*, pracodawcy korzystają z ich usług, a działania takie nie są wprost zakazane przez prawo – to można stwierdzić, że nie są z nim niezgodne. Z drugiej jednak strony z literalnej wykładni przepisu art. 22<sup>1</sup> k.p. wprost wynika, że to pracodawca ma prawo żądać podania od kandydata na pracownika konkretnych danych i w związku z tym to on, a nie jakikolwiek inny podmiot, jest ich dysponentem/administratorem. Wprawdzie np. Screening.pl nie żąda od kandydata na pracownika podania danych czy wysłania CV, kandydat robi to bowiem z własnej inicjatywy, niemniej to pracodawca jest inicjatorem, aby dane zostały przekazane dalej i to on wysyłała kandydatowi login i hasło do platformy. Ponadto z § 3 przepisu art. 22<sup>1</sup> k.p. można wywieść, że udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą, a pracodawca ma prawo żądać udokumentowania danych osobowych osób, o których mowa w § 1 i 2 tego artykułu<sup>5</sup>. Jak wskazano w piśmiennictwie, podstawowym celem przepisu jest nie tylko wskazanie podstawy żądania udostępnienia danych osobowych przez pracodawcę, ale również określenie granic przedmiotowych

<sup>5</sup> Zob. A.M. Świątkowski, *Kodeks pracy. Komentarz*, C.H. Beck, wyd. 5, Warszawa 2016, s. 140–143; M. Gersdorf, *Kilka uwag praktycznych o ochronie danych osobowych pracownika*, „Praca i Zabezpieczenie Społeczne” 2005, nr 8, s. 14–19.

tego uprawnienia, które uniemożliwia w ten sposób ewentualne nadużycia<sup>6</sup>. W mojej ocenie k.p. wyraźnie więc zakreśla zakres podmiotowy omawianej regulacji. „Prześwietlanie” kandydata przez podmiot trzeci na wyraźne żądanie pracodawcy i to z zastrzeżeniem, że jeżeli kandydat nie wyrazi na to zgody, nie będzie możliwe przejście procesu rekrutacji, budzi moje wątpliwości, gdyż mogłoby stanowić o bezpodstawnym pozbawieniu kandydata prawa do swobodnie wybranej pracy, naruszając tym samym zasadę wolności pracy oraz zasady współżycia społecznego i społeczno-gospodarcze przeznaczenie prawa. Słuszną była propozycja<sup>7</sup> brzmienia przepisu art. 22<sup>2</sup> k.p., zgodnie z którym brak zgody kandydata na pracownika lub jej wycofanie w zakresie innych kategorii danych niż wymienione wprost w ustawie, nie powinno być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny odmowy zatrudnienia, wypowiedzenia umowy o pracę lub jej rozwiązania bez wypowiedzenia przez pracodawcę. Takie brzmienie przepisu nie zostało jednak wprowadzone do ustawy, podobnie jak problematyka rekrutacji. Regulacje miały być zmienione w związku z wejściem w życie RODO, jednak tak się nie stało, co stanowi o kolejnym niedostosowaniu k.p. do obecnych realiów.

## Credit check / criminal check

Jeżeli chodzi o kontrolę kredytową kandydata na pracownika (tzw. *credit check*), to trzeba stwierdzić, że w Polsce nie ma przepisów przewidujących taką procedurę. Raport kredytowy w Biurze Informacji Kredytowej (BIK) zawiera przede wszystkim informacje o zadłużeniach – obecnych i dawnych – oraz o terminowości ich spłat. Pytanie brzmi – po co pracodawcy takie informacje?

Tu znowu trzeba przywołać przepisy dotyczące możliwej kontroli, ochrony danych osobowych, k.p. oraz Konstytucji, z których wynika, że każdemu przysługuje ochrona danych go dotyczących, szczególnie danych sensytywnych (wrażliwych). Wprawdzie w art. 9 RODO historia kredytowa nie jest wskazana jako element danych wrażliwych, więc teoretycznie pracodawca może mieć do niej dostęp, jednak wątpliwa wydaje się potrzeba posiadania przez pracodawcę informacji o sytuacji finansowej i ewentualnych ciężących

<sup>6</sup> J. Stelina, *Komentarz do 22<sup>1</sup> KP*, [w:] *Kodeks pracy. Komentarz*, red. A. Sobczyk, C.H. Beck, Warszawa 2018, <https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damjzgyzdonboobqxlругi4tinbrhaza> [dostęp: 15.05.2018].

<sup>7</sup> Zgodnie z projektem z 8 maja 2018 r. ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 (RCL, UC100).

na kandydacie na pracownika wierzytelnościach, bowiem nie jest ona adekwatna i proporcjonalna do realizacji usprawiedliwionego celu. Z drugiej jednak strony, jeżeli prowadzona jest rekrutacja na wysokie stanowiska menadżerskie, szczególnie na takie, na których pracownik ma dostęp do szczególnie ważnych informacji, stanowiących wręcz *know-how* pracodawcy, gdzie podpisywana jest z pracownikami umowa o poufności czy zakazie konkurencji, nie liczy się tylko doświadczenie zawodowe i umiejętności. W dzisiejszych czasach ważne są również kompetencje miękkie oraz tzw. kręgosłup moralny, postawa, przeszłość, ocena w branży czy też nastawienie kandydata na pracownika. Ponadto pracodawcy niechętnie realizują uprawnienie wynikające z przepisu art. 87 k.p. – dotyczącego dokonywania potrąceń z wynagrodzenia – gdyż niejednokrotnie jest to dla nich niepotrzebny kłopot. Wprawdzie można by było jako podstawę prawną działania pracodawcy wskazać przepis art. 22<sup>1</sup> § 4 k.p., z którego wynika, że pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów, jednak w zakresie historii kredytowej pracownika, przy standardowych pracach, a nie np. w służbie publicznej, trudno taki przepis wskazać.

Wątpliwe wydaje się uzyskanie pisemnej zgody pracownika czy kandydata na pracownika na przeprowadzenie procedury *credit check*, można by było bowiem stwierdzić, że stanowi to obejście wskazywanego wyżej przepisu art. 22<sup>1</sup> § 1 k.p. Grupa Robocza Unii Europejskiej, w przyjętym przez siebie dokumencie z 1 sierpnia 2003 r. stwierdziła, że

pracodawca popełnia błąd, jeśli próbuje zalegalizować przetwarzanie danych pochodzących od pracownika za pomocą uzyskanej od pracownika zgody. Można posłużyć się zgodą, jeśli odnosi się ona do przypadku, w którym pracownik ma całkowitą swobodę jej udzielenia i może odmówić udzielenia takiej zgody bez poniesienia szkody<sup>8</sup>.

Uzyskanie zgody na pobranie dodatkowych danych osobowych mogłoby mieć rację bytu przy weryfikacji przeszłości kryminalnej kandydata na pracownika czy pracownika (*criminal check*), jednak też obok wyraźnego zastrzeżenia ustawowego. Zgoda sama w sobie wydaje się wątpliwa, gdyż dane o niekaralności są szczególnie chronione<sup>9</sup>. Podstawą prawną byłby każdorazowo dany przepis, pozostający *lex specialis* w stosunku do przepisu art. 22<sup>1</sup> § 4 k.p.

<sup>8</sup> Wyrok NSA z 6 września 2011 r., sygn. I OSK 1476/10, Legalis nr 369758.

<sup>9</sup> K. Wrońska-Zblewska, *Możliwość weryfikacji, czy kandydat na pracownika nie był karany w przypadku uzyskania zgody na przetwarzanie tych danych*, Legalis, <https://sip.legalis.pl/document-full.seam?documentId=mjuwelrsga2tcmbuhe4dk> [dostęp: 15.05.2018].

– tam, gdzie obowiązuje wymóg niekaralności<sup>10</sup>. W myśl przepisu art. 6 ust. 1 pkt 10 ustawy z 24 maja 2000 r. o Krajowym Rejestrze Karnym<sup>11</sup>, prawo do uzyskania informacji o osobach, których dane osobowe zgromadzone zostały w Rejestrze, przysługuje pracodawcom, w zakresie niezbędnym dla zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej. Zatem pracodawca nie ma potrzeby, a nawet prawa posiadania informacji o niekaralności w stosunku do każdej grupy pracowników, a tylko do takiej, co do której *expressis verbis* jest to określone w ustawie szczególnej.

Ponadto zgodnie z przepisem art. 10 RODO przetwarzania danych osobowych dotyczących wyroków skazujących i naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

Podsumowując ten zakres problematyki, kontrola nie może oczywiście naruszać przepisów k.p., RODO, ustawy z 10 maja 2018 r. o ochronie danych osobowych<sup>12</sup>, dóbr osobistych, godności, prawa do prywatności – czyli wartości konstytucyjnych, które tak bardzo są ostatnio chronione (szczególnie po wejściu w życie RODO) – ani prowadzić do dyskryminacji. Główna regulacja ograniczająca w mojej ocenie możliwość kontroli i prześwietlania kandydata na pracownika czy pracownika przez pracodawcę wynika z przepisu art. 8 ust. 1 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z 4 listopada 1950 r.<sup>13</sup>, zgodnie z którym każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Powszechna Deklaracja Praw Człowieka<sup>14</sup> w przepisie art. 12, Międzynarodowy Pakt Praw Obywatelskich i Politycznych<sup>15</sup> w przepisie art. 17 ust. 1 i 2 również poruszają niniejsze zagadnienie. Ponadto

<sup>10</sup> Np. w przypadku zatrudnienia nauczyciela mianowanego, pracownika służby cywilnej, członka zarządu banku, funkcjonariusza publicznego.

<sup>11</sup> Tekst jedn.: Dz.U. z 2018 r., poz. 730.

<sup>12</sup> Dz.U. z 2018, poz. 1000 (dalej: ustawa).

<sup>13</sup> Dz.U. z 1993, nr 61, poz. 284.

<sup>14</sup> Powszechna Deklaracja Praw Człowieka, uchwalona 10 grudnia 1948 r., [http://www.unesco.pl/fileadmin/user\\_upload/pdf/Powszechna\\_Deklaracja\\_Praw\\_Czlowieka.pdf](http://www.unesco.pl/fileadmin/user_upload/pdf/Powszechna_Deklaracja_Praw_Czlowieka.pdf) [dostęp: 15.05.2018].

<sup>15</sup> Dz.U. z 1977 r., nr 38, poz. 167.

przepis art. 47 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.<sup>16</sup> mówi, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Wyżej sformułowane prawo do prywatności<sup>17</sup> uzupełniają przepisy odnoszące się do ochrony tajemnicy komunikowania się i prawa jednostki do ochrony danych osobowych. Są to prawa niekwestionowane, które muszą być respektowane nie tylko przez władze publiczne, ale i inne podmioty, skuteczne *erga omnes*<sup>18</sup>.

Trybunał Konstytucyjny w uzasadnieniu wyroku<sup>19</sup>, stwierdził, że w zakresie art. 51 Konstytucji prawodawca konstytucyjny kładzie nacisk przede wszystkim na ochronę jednostki wobec władz publicznych, bowiem to jest podmiot, który zobowiązany jest do realizacji prawa jednostki do nieuwajniania inaczej niż na podstawie ustawy informacji dotyczących swojej osoby. Trybunał dodał jednak, że wymieniony przepis konstytucyjny dotyczy wszelkich przypadków, w których jednostka zobowiązana zostaje do ujawniania informacji o sobie innym podmiotom, a więc także podmiotom prywatnym.

### *Dane biometryczne*

W Polsce coraz popularniejsza staje się identyfikacja osób za pomocą danych biometrycznych. Czym jest biometria? Słowo pochodzi z języka greckiego, gdzie *bios* oznacza 'życie', a *metron* – 'mierzyć', tak więc jest to technika dokonywania pomiarów istot żywych. Pomiary mogą być wykonywane w różny sposób, poprzez odniesienie się do konkretnych cech, m.in. cech fizycznych (np. tęczęwka, linie papilarne, układ naczyń krwionośnych na dłoni lub przebieg ręki, rozkład punktów i temperatur na twarzy, DNA), a także cech behawioralnych (np. głos, sposób chodzenia, podpis odręczny, dynamika i sposób pisanie na klawiaturze). Dane biometryczne wymienione są wprost w RODO jako szczególna kategoria danych osobowych: przepis art. 9 ust. 1 rozporządzenia zabrania przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego

<sup>16</sup> Dz.U. z 2009 r., nr 114, poz. 946 (dalej: Konstytucja).

<sup>17</sup> Zob. T. Liszcz, *Ochrona prywatności pracownika w relacjach z pracodawcą*, „Monitor Prawa Pracy” 2007, nr 1, s. 9–15.

<sup>18</sup> P. Litwiński, *Publicznoprawna ochrona danych osobowych jako środek ochrony prywatnej*, [w:] *Dobra osobiste XXI wieku. Nowe wartości, zasady, technologie*, red. J. Balcarczyk, Lex a Wolters Kluwer business, Warszawa 2012, s. 505–520.

<sup>19</sup> Wyrok TK z 19 lutego 2002 r., sygn. U3/01, OTK-A 2002, nr 1, poz. 3.

zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. W związku z faktem, że RODO weszło w Polsce w życie, jest to prawo powszechnie obowiązujące.

W związku z powyższym, kluczowe dla przedmiotowej kwestii pozostaje to, że przetwarzanie danych biometrycznych, jak i innych danych wrażliwych, co do zasady jest zabronione. Co do zasady, ponieważ istnieją regulacje, które dopuszczają przetwarzanie tych danych. I tak, przepis art. 9 ust. 2 RODO wskazuje, że nie jest zabronione przetwarzanie szczególnych kategorii danych osobowych, jeżeli jest spełniony chociaż jeden z ustawowych wyjątków. Taki, który odnosi się do stosunku pracy, jest wyrażony w pkt b): przetwarzanie jest dozwolone, jeżeli jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą.

O danych biometrycznych *expressis verbis* mowa w przepisie art. 2 pkt 1 ustawy o dokumentach paszportowych z 13 lipca 2006 r.<sup>20</sup>. Zgodnie z nim przez dane biometryczne należy rozumieć wizerunek twarzy i odciski palców umieszczone w dokumentach paszportowych w formie elektronicznej. Ustawodawca zastrzegł więc możliwość pobierania danych biometrycznych w celu wydania tzw. paszportu biometrycznego, który pozwala zidentyfikować tożsamość na podstawie danych cech fizycznych.

W odniesieniu do biometrii w prawie pracy, to można jej dokonywać na różne sposoby, m.in. w celu weryfikacji tożsamości. Najbardziej popularną formą jest „odcisk palca”, zatem skanowanie linii papilarnych, które przybierają następnie postać cyfrową. Ma to zastąpić kartę dostępu – uniemożliwiać wejście na teren zakładu pracy osób nieuprawnionych i fałszowanie rzeczywistego czasu pracy przy pomocy innych osób, stanowić o kontroli dostępu do pomieszczeń, sprzętu służbowego, zbioru danych, dokumentów, programów oraz ułatwiać prowadzenie ewidencji czasu pracy.

„Niewątpliwie wykorzystywanie danych biometrycznych w zakładach pracy to przyszłość. Przyszłość, od której ani pracownicy, ani pracodawcy nie uciekną”<sup>21</sup> – słowa sprzed dekady się sprawdziły, jednak nadal sytuacja

<sup>20</sup> Dz.U. z 2018 r., poz. 1919.

<sup>21</sup> K. Malik, *Problematyka przetwarzania danych biometrycznych pracowników*, „Monitor Prawa Pracy” 2008, nr 12, <https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogqy-damzyg43dm#> [dostęp: 17.05.2018].



prawna danych biometrycznych nie została uregulowana. *De lege ferenda*, pozyskiwanie danych biometrycznych być może mogłoby być dozwolone na szerszą skalę, jeżeli byłoby wykorzystywane w celu ochrony szczególnych interesów pracodawcy, np. zapewnienia bezpieczeństwa pracowników lub ochrony mienia, kontroli produkcji, zachowania w tajemnicy poufnych informacji czy systemów. Zatem ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony. Mogłoby być też dopuszczalne, gdyby podanie takich danych było niezbędne do wypełnienia przez pracodawcę obowiązku nałożonego przepisem prawa. Do przetwarzania takich danych powinni być wówczas dopuszczeni wyłącznie pracownicy posiadający pisemne upoważnienie nadane przez pracodawcę oraz obowiązani do zachowania tajemnicy. Sytuacja prawna pracowników w zakresie pozyskiwania ich danych osobowych (szczególnie wrażliwych) nadal nie jest wprost i czytelnie uregulowana w polskim ustawodawstwie. Ogromną szansą – niewykorzystaną niestety przez ustawodawcę – na wypełnienie tej luki prawnej była nowelizacja wynikająca z wejścia w życie RODO.

Konkludując w tym zakresie, przetwarzanie danych biometrycznych stanowi o kontroli ze strony pracodawcy. Niezależnie od tego, iż w maju 2018 r. k.p. został znowelizowany i po raz pierwszy w polskim prawie pracy została wprost uregulowana możliwość kontroli pracownika przez pracodawcę<sup>22</sup>, to nadal kontrola ta nie jest nieograniczona. W mojej ocenie nieprzekraczalną granicą kontroli jest godność człowieka, jego wolność i prywatność. Nie powinno to działać *a casu ad casum*. Zresztą przepis art. 30 Konstytucji potwierdza, że przyrodzona i niezbywalna godność człowieka stanowi źródło wolności i praw człowieka i obywatela. Nikt nie ma prawa nikogo uprzedmiotowić, nawet za jego wyraźną zgodą – niekiedy jest ona bowiem wątpliwa i nie zawsze nieprzymuszona. Prawo powinno podążać za technologią, ale postęp technologiczny musi być zgodny z nadrzędnymi wartościami. Próbuje powyższemu nadać wymiar aksjologiczny, rozpatrywany nie tylko w ramach norm prawnych, a także w kontekście etyki. Dane w formie cyfrowej przechowywane w bazach danych mogą być przecież nielegalnie wykorzystywane do różnych celów, np. udostępniane nieuprawnionym podmiotom<sup>23</sup> zajmującym się kupowaniem danych biometrycznych czy co gorsza użyte w celu

<sup>22</sup> Dotychczas uregulowana była kontrola telepracownika, a także bieżące kierownictwo pracodawcy i podporządkowanie pracownika.

<sup>23</sup> Zob. M. Korga, *Dane biometryczne i ich wykorzystywanie na gruncie stosunku pracy*, „Monitor Prawa Pracy” 2011, nr 12, <https://sip.legalis.pl/document-full.seam?documentId=mjxw-62zoge2dambuhaydqng> [dostęp: 17.05.2018].

przygotowania ataków terrorystycznych, poprzez tzw. kradzież tożsamości. Łatwo też może dojść do wycieku danych, jeżeli nie są odpowiednio zabezpieczone.

Generalizując, wszelkie dane osobowe powinny być przetwarzane zgodnie z prawem, zbierane dla oznaczonych i adekwatnych celów oraz niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Dane biometryczne są też wykorzystywane przy badaniach poligraficznych kandydatów na pracowników czy pracowników w toku zatrudnienia<sup>24</sup>. NSA stwierdził w wyroku, iż „skutki badań poligraficznych, mimo że dobrowolnych, naruszają prawa i wolności osobiste badanych. Wyrażenie zgody na badania przy pomocy wykrywacza kłamstw, prowadzone przez pracodawcę, stawia pod znakiem zapytania swobodę tej decyzji”<sup>25</sup>.

Za brakiem możliwości wykorzystywania danych biometrycznych (gdzie nie jest to przewidziane przepisami, por. motyw 52 RODO, który wskazuje, że należy również zezwolić na wyjątki od zakazu przetwarzania szczególnych kategorii danych osobowych), przemawia regulacja o charakterze ogólnym, tj. art. 11<sup>1</sup> k.p., w myśl którego pracodawca jest obowiązany szanować godność i inne dobra osobiste pracownika. „Dobrami osobistymi są powszechnie uznane w społeczeństwie wartości niemajątkowe związane ściśle z osobą człowieka i będące przejawami godności osoby ludzkiej, obejmujące przede wszystkim integralność fizyczną i psychiczną oraz indywidualność człowieka”<sup>26</sup>. Do dóbr osobistych z art. 23 k.c.<sup>27</sup> w omawianym zakresie zalicza się m.in. prawo do prywatności, godność, dane biometryczne oraz wizerunek.

<sup>24</sup> К. Пивоварска, *Полиграфное тестирование в трудовом праве – что не запрещено, то разрешено?* [K. Piwowarska, *Badania poligraficzne w prawie pracy – co nie jest zakazane, jest dozwolone?*], [w:] *Применение полиграфа в бывшем восточном блоке*, pod red. Я. Видацкого, В. Шаповалова, И. Усикова [Badania poligraficzne w byłym bloku wschodnim, red. J. Widacki, V. Shapovalov, I. Usikov], Oficyna Wydawnicza AFM, Kraków 2017, s. 171–188; por. A. Drozd, *O dopuszczalności wykorzystywania wariografu w stosunkach pracy*, „Praca i Zabezpieczenie Społeczne” 2003, nr 4, s. 9–14; M. Leśniak, M. Gramatyka, *Dopuszczalność badań poligraficznych w świetle konstytucyjnych praw i wolności obywatelskich*, „Prawa Człowieka” 1998, nr 5, s. 141–152; A. Cempura, M. Widacki, *Prawna dopuszczalność pracowniczych badań poligraficznych w Polsce*, „Palestra” 2012, nr 11–12, s. 39–47; J. Pietruszka, R. Rogalski, *Nie odbierać prawa do obrony – artykuł dyskusyjny o poligrafie*, „Praca i Zabezpieczenie Społeczne” 2004, nr 11, s. 15–21; R. Jaworski, *Badania poligraficzne (wariograficzne) w ochronie miejsce pracy*, „Praca i Zabezpieczenie Społeczne” 2007, nr 1, s. 11–15.

<sup>25</sup> Wyrok NSA z 13 lutego 2003 r., sygn. II SA 1620/01.

<sup>26</sup> *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, wyd. 8, C.H. Beck, Warszawa 2017, <https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damjxgazdknroobqxlrugmydqnzrgy3q> [dostęp: 18.05.2018].

<sup>27</sup> Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, tekst jedn.: Dz.U. z 2018 r., poz. 1025.

NSA w wyroku z 1 grudnia 2009, sygn. I OSK 249/09<sup>28</sup> stwierdził, że brak równowagi w relacji pracodawca–pracownik stawia pod znakiem zapytania dobrowolność wyrażenia zgody na pobieranie i przetwarzanie danych osobowych (biometrycznych). Z tego względu ustawodawca ograniczył przepisem art. 22 k.p. katalog danych, których pracodawca może żądać od pracownika. Ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. W przypadku wykorzystania danych biometrycznych do kontroli czasu pracy pracowników takie ryzyko jest nieproporcjonalne do zamierzonego celu przetwarzania.

Podobne stanowisko zaprezentował NSA w wyroku z 6 września 2011 r., sygn. akt I OSK 1476/10<sup>29</sup>. Natomiast WSA w Warszawie w wyroku z 20 czerwca 2011 r., sygn. akt SA/Wa 719/11<sup>30</sup> wskazał, że pracodawca popełnia błąd, jeśli próbuje zalegalizować przetwarzanie danych pochodzących od pracownika za pomocą uzyskanej od pracownika zgody. Można posłużyć się zgodą, jeśli odnosi się ona do przypadku, w którym pracownik ma całkowitą swobodę jej udzielenia i może odmówić udzielenia takiej zgody bez poniesienia szkody. W tym zakresie podobnie wypowiedział się również GODO w decyzji z 15 grudnia 2009 r.<sup>31</sup>, w której nakazał usunięcie przedsiębiorcy danych osobowych, obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników, przetwarzanych w celu ewidencji czasu pracy, oraz zaprzestanie zbierania ww. danych osobowych. Jeżeli więc istnieją inne sposoby kontroli czasu pracy, np. karty czy wpis do dziennika, to należy w pierwszej kolejności wykorzystać te, które nie naruszają prywatności pracownika.

WSA w wyroku z 18 czerwca 2010, sygn. II SA/Wa 151/10<sup>32</sup>, stwierdził, że wyrażona na prośbę pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie jego danych osobowych narusza prawa pracownika i swobodę wyrażenia przez niego woli. Tak więc skoro pracownik nie inicjuje podania tych danych, a zwraca się o nie pracodawca, to trudno mówić o dobrowolnej i swobodnej zgodzie, tym bardziej że już z samego art. 22 k.p. wynika stosunek podrzędności i kierownictwa ze strony pracodawcy, bowiem osoba,

<sup>28</sup> ONSAiWSA 2011, nr 2, poz. 39, s. 169.

<sup>29</sup> LEX nr 965912. Zob. E. Kulesza, *Glosa do wyroku NSA z dnia 6 września 2011 r.*, I OSK 1476/10, OSP 2013/10/104.

<sup>30</sup> LEX nr 994017.

<sup>31</sup> Decyzja GODO z 15 grudnia 2009 r. nakazująca usunięcie przedsiębiorcy danych biometrycznych – odcisków palców – ze zbioru prowadzonego w celu ewidencji czasu pracowników, DIS/DEC-1261/46988/09 dot. DIS-K-421/138/09, <https://giodo.gov.pl/pl/289/3336> [dostęp: 15.05.2018].

<sup>32</sup> LEX nr 643811.

której dane dotyczą, pozostaje w układzie podległości względem podmiotu, któremu zgoda ma być udzielona<sup>33</sup>.

Jednak nawet gdyby nie opierać się na powyższym, to przepis art. 22<sup>1</sup> § 1 k.p. taksatywnie wskazuje, jakich informacji można żądać od kandydata do pracy. Nie wskazano tam, że pracodawca może domagać się od osoby ubiegającej się o zatrudnienie jakichkolwiek danych wrażliwych. Skoro tak, to ich przetwarzanie co do zasady jest niedozwolone. Co do zasady, gdyż podobnie jak przy weryfikacji historii kryminalnej czy badaniu poligraficznym, są wyjątki ustawowe, które na to pozwalają. Odnosi się do tego przepis art. 22<sup>1</sup> § 5 k.p., zgodnie z którym w zakresie nieuregulowanym w § 1–4 do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy o ochronie danych osobowych. Co ciekawe, Sąd Najwyższy w wyroku z 5 sierpnia 2008 r., sygn. I PK 37/08<sup>34</sup>, wskazał, że polecenie pracodawcy nakładające na pracownika obowiązek udzielenia informacji (danych osobowych) niewymienionych w art. 22<sup>1</sup> § 1 i 2 k.p. lub w odrębnych przepisach (art. 22<sup>1</sup> § 4 k.p.) jest niezgodne z prawem (art. 100 § 1 k.p.) i dlatego odmowa jego wykonania nie może stanowić podstawy rozwiązania umowy o pracę w trybie art. 52 § 1 pkt 1 k.p. Nie może więc dla pracownika wywoływać negatywnych konsekwencji jego zachowanie polegające na odmowie udzielenia informacji, których nie wymaga od niego ustawa. Po raz kolejny widać więc, jak mocno działa funkcja ochronna prawa pracy w odniesieniu do pracownika.

### ***Biochipy – kontrolowanie pracowników za pomocą technologii identyfikacji radiowej (RFID)***

Według mnie dozwoloną granicę pozyskiwania danych biometrycznych przekracza również RFID (*Radio-Frequency Identification*), tzw. technologia bliskiego odczytu<sup>35</sup>. Jest to system kontroli, który wykorzystuje do komunikacji fale radiowe, dzięki mikrourządzeniom elektronicznym, nazywanym znacznikami (tagami, transponderami, chipami)<sup>36</sup>.

<sup>33</sup> P. Fajgielski, *Zgoda na przetwarzanie danych*, [w:] *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, red. G. Sibiga, X. Konarski, Oficyna a Wolters Kluwer business, Warszawa 2007, s. 47.

<sup>34</sup> OSNP 2010/1-2/4.

<sup>35</sup> Za autora metody uważa się Thomasa W. Heetera, który w marcu 1999 r. w Houston opatentował swój wynalazek (patent nr 5.878.155) i nadał mu następujący opis: „Sposób weryfikacji ludzkiej tożsamości podczas uczestniczenia w elektronicznej transakcji handlowej”.

<sup>36</sup> Zob. J. Terstegge, *Komentarz*, [w:] *Prawo do prywatności – prawo do godności*. 26. Międzynarodowa Konferencja Ochrony Prywatności i Danych Osobowych, 14–16 września 2004 Polska, Wrocław, Biuro Generalnego Inspektora Ochrony Danych Osobowych, Warszawa 2006, s. 99–101.

Transponder RFID to radiowe urządzenie nadawcze lub nadawczo-odbiorcze, które wysyła sygnał zawierający kodowane dane identyfikacyjne, ale tylko w odpowiedzi na pobudzenie sygnałem radiowym o określonej częstotliwości. Mikroprocesory emitują jednoznacznie identyfikowany numer w momencie pobudzenia radiowym sygnałem pochodzącym z czytnika. Pozwala to na identyfikację i śledzenie przedmiotów (biochip-implant pozwala zrealizować te funkcje w stosunku do żywych organizmów) także dlatego, że znaczniki te są niewielkie (znaczniki mogą być wielkości ziarnka piasku i działać bez baterii; są też znaczniki większe, mające własny system zasilania i większy zasięg transmisji)<sup>37</sup>.

Informacje zawarte w chipie są zaszyfrowane i mogą być dostępne przez fizyczne zbliżenie do czytnika, z kolei chip RFID może być zamontowany w samochodzie, na ubraniu, w karcie, ale również wszczepiony w ludzkie ciało – taki implant jest tzw. biochipem. W literaturze przedmiotu pisze się, że aktualnie jedną z „najnowocześniejszych metod kontroli pracowników jest wykorzystanie technologii identyfikacji radiowej – RFID. [...] Technologia RFID stanowi kompilację geolokalizacji z technologią biometryczną”<sup>38</sup>.

Biochipy są udoskonalonymi kodami kreskowymi – istnieje inna metoda identyfikacji, tj. wytatuowanie na ręce lub czoło znaku w formie kodu kreskowego. Taki tatuaż zawiera dane personalne potrzebne do ustalenia tożsamości podmiotu.

W 2015 r. jeden ze szwedzkich pracodawców, firma Epicenter, zdecydował się na wszczepienie pracownikom, którzy dobrowolnie się na to zgodzili, biochipów. Pracownicy poprzez przyłożenie ręki do czytnika mogą dostawać się do pomieszczeń i zbiorów danych, kopiować i skanować dokumenty, odbierać telefony, łączyć się z Internetem, robić zakupy online, a nawet płacić w sklepie.

Oczywiście nie kwestionuję przydatności nowych technologii – choćby do odnajdywania porwanych lub zaginionych osób (np. chorych na chorobę Alzheimera) czy monitorowania więźniów – ani możliwości ich zastosowania w medycynie – np. do badań czy usprawniania organizmu (rozzrusznik serca, aparat słuchowy), jednak w stosunkach pracy jej zastosowanie wydaje się niepotrzebne, a w realiach polskich – wręcz zabronione. Pracodawca byłby w stałym posiadaniu informacji na temat pracownika, szczególnie o jego lokalizacji, przez co mógłby go nieustannie kontrolować, a wręcz inwigilować. W tym zakresie praca ludzka nie może więc zostać zalgorytmizowana. Biochipy, skoro stają się nierozdzielalnym elementem ludzkiego ciała, naruszają

<sup>37</sup> K.M. Szymorek, *Aspekty prawne kontrolowania pracowników za pomocą technologii identyfikacji radiowej (RFID)*, „Monitor Prawa Pracy” 2012, nr 10, <https://sip.legalis.pl/document-full.seam?documentId=mjxw62zoge2dkmbvge2dcmy> [dostęp: 15.05.2018].

<sup>38</sup> *Ibidem*.

nadrzędne wartości, o których pisałam wyżej. Z korzystania z czytnika linii papilarnych można zrezygnować w każdym momencie, a z biochipa – już niekoniecznie.

### *Zawody zagrożone wyparciem z rynku i zawody przyszłości*

Należy zadać sobie pytanie, czy w związku ze zmianami globalizacyjnymi i rozwojem technologicznym istnieją zawody zagrożone wyparciem z rynku pracy, oraz *a contrario* – zawody przyszłości.

Według raportu *Aktywni+. Przyszłość rynku pracy*<sup>39</sup> serwisu Gumtree.pl, 40% miejsc pracy w Polsce zastąpią w przyszłości roboty i maszyny. Nowe technologie, w tym maszyny, już wyparły z rynku pracy wielu pracowników – szczególnie w fabrykach. Stało się tak, ponieważ praca człowieka okazała się bardziej zawodna i mniej opłacalna niż praca zautomatyzowanych robotów. Maszyna jest szybsza, dokładniejsza oraz mniej kłopotliwa – poza bieżącym serwisem nie potrzebuje przerw w pracy, nie żąda podwyżki, nie dotyczy jej minimalna stawka wynagrodzenia, nie bierze urlopu na żądanie czy zwolnienia chorobowego. Człowiek okazuje się więc mniej wydajny. Jednak czy każdą pracę da się zautomatyzować? Wydaje się, że nie, a nawet jeśli się dało, to nie byłoby to słuszne. Zgodnie z raportem, za około 25 lat cyfryzacja i automatyzacja doprowadzi do tego, że najbardziej pożądanymi i najlepiej opłacanymi zawodami będą te, w których pracuje się na dużych zbiorach danych, w tym danych statystycznych. Konieczna będzie ich analiza i interpretacja celem otrzymania wyników. W związku z tym jeszcze bardziej rozwinie się branża IT i robotyka. Na łatwe znalezienie pracy będą mogli liczyć inżynierzy, programiści i developerzy (*data scientist*, *DevOps engineer* oraz *data engineer*), pracujący nad analizą danych, tworzeniem programów i aplikacji oraz rozwojem sztucznej inteligencji. Niewątpliwie muszą to być osoby z wysokim wykształceniem, wykwalifikowane i z odpowiednim doświadczeniem. Pomimo tego i tak istnieją już boty – programy wykonujące określone czynności (np. w zakresie programowania) w zastępstwie pracownika.

Z kolei według raportu Warszawskiego Instytutu Studiów Ekonomicznych *Czy robot zabierze Ci pracę? Sektorowa analiza komputeryzacji i robotyzacji europejskich rynków pracy*<sup>40</sup> w Polsce najbardziej zagrożonymi zawodami

<sup>39</sup> *Aktywni+. Przyszłość rynku pracy. Raport Gumtree 2017*, [http://www.delab.uw.edu.pl/wp-content/uploads/2017/04/DELabUW\\_raport\\_Aktywni.pdf](http://www.delab.uw.edu.pl/wp-content/uploads/2017/04/DELabUW_raport_Aktywni.pdf) [dostęp: 15.05.2018].

<sup>40</sup> *Czy robot zabierze Ci pracę? Sektorowa analiza komputeryzacji i robotyzacji europejskich rynków pracy*, Warszawski Instytut Studiów Ekonomicznych, Warszawa, [b.d.], [http://wise-europa.eu/wp-content/uploads/2016/03/PolicyWorking-WISE-\\_nr1\\_141029.pdf](http://wise-europa.eu/wp-content/uploads/2016/03/PolicyWorking-WISE-_nr1_141029.pdf) [dostęp: 15.05.2018].

są robotnicy przetwórstwa spożywczego, pracownicy administracji, pracownicy obrotu pieniężnego, sprzątaczkę, robotnicy budowlani, górnicy, a także kolejarze, kasjerzy i kierowcy ciężarówek. Najmniej perspektywiczne, a wręcz wymierające są następujące profesje: doradca klienta bankowego, pracownicy wywołujący zdjęcia i operatorzy maszyn procesu fotograficznego, sporządzający sprawozdania podatkowe, agenci cargo i przewozu, zegarmistrzowie, agenci ubezpieczeniowi, technicy matematycy, krawcy, wyszukiwacze tytułów, telemarketerzy. Mówi się też, o możliwości zastąpienia pracy sędziów przez roboty<sup>41</sup>. Wydaje się to bardzo abstrakcyjne, aczkolwiek możliwe.

Carl B. Frey i Michael A. Osborne, naukowcy z Uniwersytetu Oksfordzkiego, opublikowali w 2013 r. wyniki pracy na projekcie *The future of employment: How susceptible are jobs to computerisation?*<sup>42</sup>. W raporcie można znaleźć zawody zagrożone wyeliminowaniem przez komputeryzację i automatyzację. Wprawdzie badania odnoszą się do krajów najbardziej rozwiniętych gospodarczo, w tym USA i krajów anglosaskich, niemniej jednak mogą stanowić pewien wyznacznik dla Polski. Według naukowców istnieją trzy czynniki, które zapobiegają automatyzacji i zbytniemu wkraczaniu technologii w rynek pracy. Są to ludzkie cechy i umiejętności: kreatywność, inteligencja społeczna oraz zdolności skutecznego zarządzania zadaniami. Dzięki temu zawody takie jak: terapeuci rekreacyjni, kierownicy zespołów: mechaników, monterów, serwisantów, dyrektorzy zarządzający sytuacjami kryzysowymi, pracownicy ochrony zdrowia psychicznego i terapii odwykowych, terapeuci zajęciowi, protetycy, pracownicy pomocy społecznej, chirurdzy jamy ustnej i twarzowo-szczękowi, dowódcy w straży pożarnej i służbach bezpieczeństwa – nie są zagrożone „wyginięciem” w ciągu najbliższych 20 lat. Na liście zamieszczono 702 zawody (im niższa pozycja na liście, tym większe prawdopodobieństwo komputeryzacji danego zawodu) – dla przykładu na 123. miejscu byli pisarze, na 144. lekarze i pielęgniarki (z zastrzeżeniem, że lekarze chirurdzy znaleźli się na 15. pozycji), na 333. rzeźnicy, a na 353. sędziowie prawa administracyjnego. Na 424. miejscu pomywacze, na 453. zarządcy nieruchomości komunalnych i prywatnych, na 505. tapetiarze, 541. rzeczoznawcy nieruchomości, a na 677. analitycy kredytowi.

<sup>41</sup> *AI zastąpi także sędziów?*, [http://www.geekweek.pl/news/2017-03-23/ai-zastapi-takze-sedziow\\_1661209/](http://www.geekweek.pl/news/2017-03-23/ai-zastapi-takze-sedziow_1661209/) [dostęp: 15.05.2018].

<sup>42</sup> C.B. Frey, M.A. Osborne, *The future of employment: How susceptible are jobs to computerisation?*, September 17, 2013, [https://www.oxfordmartin.ox.ac.uk/downloads/academic/The\\_Future\\_of\\_Employment.pdf](https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf) [dostęp: 15.05.2018].

## Uberyzacja zatrudnienia, ICT based work, crowd employment

Paczkomaty, pralniomaty, dostawa dronami, drukarki 3D, hologramy, aplikacje mobilne – wszystko to wpływa na zmianę naszego życia i konsumpcjonizm. Rozwój technologii zaspokaja potrzeby społeczne młodego „cyberpokolenia”, nazywanego iPokoleniem. Wyrażna jest ogólna tendencja do digitalizacji usług, które dostarczane są drogą internetową, a co za tym idzie – do rozwoju technologii.

I tak, w związku z rozwojem aplikacji mobilnych, coraz mniej przydatny może okazać się np. zawód taksówkarza. Aplikacja Traficar, dzięki której można krótkoterminowo wynająć auto, jest niezwykle popularna w Polsce. Podobnie Uber czy Lyft, aplikacje, która niejako zastępuje tradycyjne korporacje taksówkarskie. Wystarczy w aplikacji jeden dotyk, a samochód już jedzie, gdyż system szybko lokalizuje pasażera<sup>43</sup>. Nie ma konieczności wykonywania tradycyjnych połączeń telefonicznych i długiego oczekiwania. Analogicznie działają Deliveroo czy Uber Eats – realizujące usługę dostarczania jedzenia.

Wzrost popularności samozatrudnienia i świadczenia usług, np. przewozu na żądanie nazwano „uberyzacją zatrudnienia”<sup>44</sup>. Jest to tzw. praca na życzenie za pośrednictwem aplikacji (*work on demand via apps*). Praca taka najczęściej jest świadczona w transporcie, przy sprzątanii, załatwianiu drobnych sprawunków, a nawet przy pracach biurowych<sup>45</sup>. Używam tu słowa „praca”, ale niewątpliwie nie jest ona wykonywana w warunkach k.p., a osoby ją świadczące nie są pracownikami w rozumieniu art. 2 k.p. „Uberyzacja zatrudnienia” prowadzi do: braku stabilności zatrudnienia (dorywczości) i należyte

<sup>43</sup> Pomimo powyższych ułatwień specjaliści z Google’a, Tesli i Ubera pracują nad w pełni autonomicznymi samochodami. Prowadzone testy wykazują, że takie rozwiązanie może być nawet bezpieczniejsze niż jazda samochodem kierowanym przez człowieka.

<sup>44</sup> Jak pisze Uber na swojej stronie: „Stań się swoim własnym szefem i zarabiaj, jeżdżąc, kiedy chcesz, ile chcesz”, *Zarejestruj się, aby zostać kierowcą*, Uber, [Spośród krajów europejskich Uber cieszy się największą popularnością w Wielkiej Brytanii, Francji i Polsce. Działalność gospodarcza aplikacji we Włoszech została zakazana, we Francji – częściowo ograniczona, w Wielkiej Brytanii – częściowo uregulowana, a w Polsce pozostaje zupełnie nieuregulowana.](https://www.uber.com/al/join?ec_exp=1&exp=70801t&city=krakow&utm_source=AdWords_Brand&utm_campaign=search-google-brand_139_495_pl-krakow_d_txt_acq_cpc_pl-pl_%2Buber_kwd-38545560932_148380348625_23031856822_b_c_track-oct10urlupdate_restructure&cid=380214862&adg_id=23031856822&fi_id=&match=b&net=g&dev=c&dev_m=&cre=148380348625&kwid=kwd-38545560932&kw=%2Buber&placement=&tar=&ds_rl=[dostęp: 15.05.2018].</a></p></div><div data-bbox=)

<sup>45</sup> J. Unterschütz, *Praca w ramach platform i aplikacji cyfrowych – wyzwania dla zbiorowego prawa pracy*, cz. 1, „Monitor Prawa Pracy” 2017, nr 8, <https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damjwhaztqni> [dostęp: 20.05.2018].



ochrony, braku możliwości korzystania z pracowniczych praw indywidualnych i zbiorowych – jak prawo do godziwego wynagrodzenia, bezpieczeństwa i higieny pracy, ochrony prywatności, strajku – ponadto do przeniesienia ryzyka na świadczącego usługi, fragmentaryzacji pracy, nieuczciwej konkurencji oraz nienależitych i niewystarczających gwarancji świadczeń z ubezpieczeń społecznych<sup>46</sup>. Jednak z drugiej strony nie wolno nikomu odbierać wolności do pracy swobodnie wybranej, w tym – do samozatrudnienia.

Godne uwagi jest to, że Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy (Eurofound) wskazała nowe formy zatrudnienia – dwie postaci pracy w gospodarce cyfrowej: pracę z zastosowaniem technologii informacyjno-telekomunikacyjnych (*ICT based mobile work*) oraz *crowd employment* (w tym pracę w ramach platform cyfrowych)<sup>47</sup>.

Praca z zastosowaniem technologii informacyjno-telekomunikacyjnych definiowana jest jako sposób organizacji pracy, w ramach którego praca wykonywana jest co najmniej częściowo, a zarazem regularnie, poza główną siedzibą przedsiębiorstwa, niekiedy w domu pracownika z wykorzystaniem technologii informacyjno-telekomunikacyjnych w celu połączenia się z systemem komputerowym stosowanym w przedsiębiorstwie [...] może być wykonywana w każdym czasie i w każdym miejscu, nawet gdy pracownik jest w trakcie podróży. Pomimo wykorzystania nowoczesnej technologii tego rodzaju praca jest często wykonywana na podstawie typowej umowy o pracę<sup>48</sup>.

*ICT based mobile work* przypomina więc telepracę, która jest uregulowana w k.p. w przepisach art. od 67<sup>5</sup> do 67<sup>17</sup>, jednak istnieje różnica. W warunkach telepracy praca może być wykonywana regularnie poza zakładem pracy, z wykorzystaniem środków komunikacji elektronicznej w rozumieniu przepisów o świadczeniu usług drogą elektroniczną. Istnieje też pewien rodzaj podporządkowania co do czasu pracy, miejsca jej świadczenia (zwykle w domu, choćby ze względu na przepisy w zakresie BHP) oraz regulacji obowiązujących wewnątrz w zakładzie pracy. Natomiast świadczenie pracy z zastosowaniem technologii informacyjno-telekomunikacyjnych odbywa się w bliżej niesprecyzowanym miejscu, niekoniecznie w domu – zatem bez podporządkowania. Forma telepracy również podpada pod definicję pracy w ramach nowych technologii, jednak w obliczu innych form nie wydaje się już tak aktualna.

<sup>46</sup> B. Bednarowicz, „Uberyzacja zatrudnienia” – praca w gospodarce współdziałania w świetle prawa UE, „Monitor Prawa Pracy” 2018, nr 2, <https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damjygm3dqna> [dostęp: 20.05.2018].

<sup>47</sup> I. Mandl *et al.*, *New forms of employment*, Eurofound, Luxemburg 2015, s. 1–2.

<sup>48</sup> J. Unterschütz, *Praca w ramach platform...*

Z kolei *crowd work* (*crowd employment*), określaną także niekiedy jako *crowdsourcing*, interpretuje się jako

pracę w ramach platform cyfrowych, rozumianą jako wykonywanie serii zadań za pośrednictwem platform cyfrowych, które umożliwiają podmiotom indywidualnym i organizacjom dostęp do nieokreślonej i nieznannej grupy innych podmiotów w celu rozwiązania określonego rodzaju problemów, zrealizowania określonych usług lub dostarczenia towarów za opłatą<sup>49</sup>.

Dochodzi więc do wymiany usług, różnego rodzaju dóbr, informacji pomiędzy podmiotami z zakresu handlu, transportu, opieki zdrowotnej czy edukacji poprzez sieć internetową<sup>50</sup>.

W obliczu powyższego w przyszłości może dojść do pogłębienia się zjawiska *humans-as-a-service* (ludzie jako usługi), a czwarta rewolucja przemysłowa (tzw. przemysł 4.0)<sup>51</sup>, gospodarka oparta na wiedzy i technologii, automatyzacji, robotyzacji, sztucznej inteligencji (*artificial intelligence*, AI) zmieni w przyszłości rynek pracy. Praca ludzka nadal będzie potrzebna, tym bardziej że technologie starzeją się i dezaktualizują. Trzeba jednak mieć też na uwadze podejście bardziej sceptyczne, mówiące o tzw. bezrobociu technologicznym – gdyż w pewnych zawodach maszyny mogą wyprzeć człowieka.

### ***RODO w prawie pracy***

W związku z wejściem w życie RODO doszło do uchwalenia nowej ustawy o ochronie danych osobowych, a wraz z nią do zmiany kilkuset innych ustaw, w tym k.p. – po art. 22<sup>1</sup> dodano art. 22<sup>2</sup> i art. 22<sup>3</sup>. Co ciekawe, przepisy tych artykułów dotyczą sytuacji prawnej, która i tak już miała miejsce w zakładach pracy. Słusznie jednak została wprost uregulowana możliwość stosowania przez pracodawcę monitoringu oraz kontroli elektronicznej poczty służbowej i innych narzędzi pracy. Możliwości inwigilacji dzięki dostępności różnorodnych urządzeń są praktycznie nieograniczone, jednak powinno się to odbywać w myśl kilku zasad: zgodności z prawem, ze względu na usprawiedliwiony cel, z zastosowaniem proporcjonalności w stosunku do celu, transparentności, spełnienia wymagań określonych w przepisach o ochronie

<sup>49</sup> *Ibidem*.

<sup>50</sup> Zob. J. Unterschütz, *Nowe formy pracy w gospodarce cyfrowej – w poszukiwaniu pracownika*, [w:] *Umowa o pracę a umowa o zatrudnienie*, red. G. Goździewicz, Wolters Kluwer, Warszawa 2018, s. 323–337.

<sup>51</sup> Zob. T. Iwański, J. Gracel, *Przemysł 4.0. Rewolucja już tu jest. Co o niej wiesz?*, Astor, [Kraków 2016], [https://www.astor.com.pl/images/Industry\\_4-0\\_Przemysl\\_4-0/ASTOR\\_przemysl4\\_whitepaper.pdf](https://www.astor.com.pl/images/Industry_4-0_Przemysl_4-0/ASTOR_przemysl4_whitepaper.pdf) [dostęp: 20.05.2018].

danych osobowych<sup>52</sup>. Istnieją obostrzenia co do stosowania kontroli – monitoring w postaci środków technicznych umożliwiających rejestrację obrazu można wprowadzić, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia, lub kontroli produkcji, lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Będzie to tzw. szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy. Ponadto monitoring nie może służyć do kontroli pracy świadczonej przez pracowników. Cele jego wprowadzenia są jasno określone (wyliczone enumeratywnie) w art. 22<sup>2</sup> § 1 k.p. Co do zasady, monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni lub pomieszczeń udostępnianych zakładowej organizacji związkowej, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celów wskazanych wyżej – oczywiście z zastrzeżeniem, że nie naruszy to godności oraz innych dóbr osobistych pracownika, a także zasady wolności i niezależności związków zawodowych. Monitoring może się odbywać przy zastosowaniu technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Takie nagrania obrazu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania, następnie zobowiązany jest je zniszczyć. Co ważne, w związku z powyższą regulacją zmieniły się również przepisy w zakresie źródeł prawa wewnątrzzakładowego. Postanowienie o wprowadzeniu monitoringu musi znaleźć się w układzie zbiorowym pracy, w regulaminie pracy albo w obwieszczeniu. Nie później niż na 2 tygodnie przed uruchomieniem monitoringu pracodawca jest zobowiązany powiadomić o jego wprowadzeniu pracowników. Poza powyższym obowiązkiem informacyjnym pracodawca oznacza też pomieszczenia i teren monitorowany w taki sposób, aby to było widoczne i czytelne, np. za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem. W zakresie nowo zatrudnionych pracowników, jeszcze przed ich dopuszczeniem do pracy pracodawca zobowiązany jest na piśmie przekazać im informacje o obowiązujących zasadach monitoringu.

Dozwolona jest również kontrola służbowej poczty elektronicznej pracownika, a także inne formy monitoringu, jednak ustawodawca nie wskazuje jakie. Tak więc dzięki katalogowi otwartemu można wywieść, że chodzi

<sup>52</sup> A. Lach, *Monitorowanie pracownika w miejscu pracy*, „Monitor Prawa Pracy” 2004, nr 10, <https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi2tamrzgq2tg> [dostęp: 20.05.2018]; idem, *Inwigilacja przy użyciu kamer użytkowych*, [w:] *Spółeczeństwo inwigilowane w państwie prawa*, red. P. Chrzczonowicz, V. Kwiatkowska-Darul, K. Skowroński, Wydawnictwo Uniwersytetu Mikołaja Kopernika, Toruń 2003, s. 143–150.

o kontrolę samochodu służbowego poprzez zamontowanie lokalizatora GPS, kontrolę aktywności prawnika w Internecie (np. na portalach Facebook, LinkedIn, GoldenLine), kontrolę telefonu służbowego, a nawet kontrolę osobistą, tj. przeszukiwanie w sytuacji, gdy istnieje podejrzenie czy uzasadnione podejrzenie, że pracownik wynosi z zakładu pracy mienie pracodawcy, zatem narusza podstawowe obowiązki pracownicze, w tym zasady ochrony mienia oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Powyższe jest o tyle uzasadnione, że kontrole mogą być przeprowadzone, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Czas pokaże, jak przyjmą się nowe sposoby kontroli pracowników. *De lege lata* słusznie iż ustawodawca, choć niekompletnie, ale jednak uregulował tę kwestię. Niewątpliwie brakuje doregulowania w zakresie pobierania danych biometrycznych i możliwości kontroli z tego wynikających, a także stosowania *criminal i credit check*.

Fakt funkcjonowania w Polsce coraz liczniejszych korporacji, praca na odległość, podróże służbowe oraz komunikowanie się przez środki masowego przekazu, daje wiele możliwości, aby w mądry sposób korzystać z nowych zasad kontroli pracowników. RODO w prawie pracy zostało więc wprowadzone bardziej pod kątem pracodawców, jednak nadal z poszanowaniem konstytucyjnie chronionych godności, dóbr osobistych i prawa do prywatności.

### *Podsumowanie*

Uważam, że rynek pracy już został zrewolucjonizowany przez nowe technologie. *De lege ferenda* prawo powinno nadążać za tym rozwojem, jednak z poszanowaniem nadrzędnych wartości i w zgodzie z autentyczną wolą kandydata na pracownika czy pracownika. Zastosowanie sztucznej inteligencji w stosunkach pracy powinno mieć granice. Zatem odpowiedź na pytanie, czy nowe technologie zrewolucjonizują rynek pracy – stanowczo brzmi: tak, jednak granice dopuszczalnej rewolucji zależą od woli każdego z nas.

**Abstract****Whether new technologies will revolutionize the labour market?**

The article discusses changes in the labour law in connection with globalization, automation, civilization and technological development, especially against the background of new forms of employment: „ICT based work”, „crowdworking”. It was also considered whether the use of new technologies by the employer or the future employer, including in the scope of background screening (including credit and criminal check), acquisition and use of biometric data, application of radio frequency identification technology (RFID) by implanting a chip for employee control or organizational processes improvement at the employer, does not constitute abuse of the subjective right to privacy and does not violate dignity. The above was referred to the General Data Protection Regulation of 27.04.2016 (GDPR) and related changes in the Labour Code. To determine whether new technologies will revolutionize the labour market the question was asked: are there occupations that are at risk of being forced out of the labour market due to the automation of work, and contrarily – are there professions of the future.

**Key words:** new technologies, Labour Law, General Data Protection Regulation (GDPR)

**Streszczenie****Czy nowe technologie zrewolucjonizują rynek pracy?**

W artykule poruszono temat zmian w prawie pracy w związku z globalizacją, automatyzacją, rozwojem cywilizacyjnym i technologicznym, szczególnie na tle nowych form zatrudnienia: pracy z zastosowaniem technologii informacyjno-telekomunikacyjnych (*ICT based work*) i pracy w ramach platform cyfrowych (*crowdworking*). Rozważono również, czy wykorzystywanie nowych technologii przez pracodawcę czy przyszłego pracodawcę, m.in. w zakresie *background screening* (w tym *credit* i *criminal check*), pozyskiwania i wykorzystywania danych biometrycznych, zastosowania technologii identyfikacji radiowej (RFID) poprzez wszczepianie chipa dla kontroli pracownika czy usprawnienia procesów organizacyjnych, nie stanowi nadużycia podmiotowego prawa do prywatności i wręcz nie narusza godności. Powyższe odniesiono do Ogólnego Rozporządzenia o Ochronie Danych Osobowych z 27 kwietnia 2016 r. (RODO) i związanych z nim zmian w Kodeksie pracy. Aby przesądzić, czy nowe technologie zrewolucjonizują rynek pracy, postawiono pytanie: czy istnieją zawody, które są zagrożone wyparciem z rynku ze względu na automatyzację pracy, oraz przeciwnie – czy istnieją zawody przyszłości.

**Słowa kluczowe:** nowe technologie, prawo pracy, rozporządzenie o ochronie danych osobowych (RODO)

